Reachability Probabilities of Quantum Markov Chains

Shenggang Ying, Yuan Feng, Nengkun Yu and Mingsheng Ying

Tsinghua University, China
University of Technology, Sydney, Australia
{Shenggang.Ying,Yuan.Feng,Mingsheng.Ying}@uts.edu.au

Abstract. This paper studies three kinds of long-term behaviours, namely reachability, repeated reachability and persistence, of quantum Markov chains (qMCs). As a stepping-stone, we introduce the notion of bottom strongly connected component (BSCC) of a qMC and develop an algorithm for finding BSCC decompositions of the state space of a qMC. As the major contribution, several (classical) algorithms for computing the reachability, repeated reachability and persistence probabilities of a qMC are presented, and their complexities are analysed.

1 Introduction

Verification problem of quantum systems are emerging from quantum physics, quantum communication and quantum computation. For example, verification has been identified by physicists as one of the major short-term goals of quantum simulation [4]. Some effective verification techniques for quantum cryptographic protocols have recently been developed [12], [6], based on either quantum process algebras [15], [11], [8], [9] or quantum model-checking [13]. Also, several methods for verifying quantum programs [20] have been proposed, including quantum weakest preconditions [7] and quantum Floyd-Hoare logic [23].

A quantum Markov chain (qMC) is a quantum generalisation of Markov chain (MC) where, roughly speaking, the state space is a Hilbert space, and the transition probability matrix of a MC is replaced by a super-operator, which is a mathematical formalism of the discrete-time evolution of (open) quantum systems. qMCs have been widely employed as mathematical model of quantum noise in physics [10] and as model of communication channels in quantum information theory [17]. A special class of qMCs, namely quantum walks, has been successfully used in design and analysis of quantum algorithms [1]. Recently, the authors [24] introduced a model of concurrent quantum programs in terms of qMCs as a quantum extension of Hart-Sharir-Pnueli's Markov chain model of probabilistic concurrent programs [14]. This paper considers the verification problem of qMCs.

Reachability analysis is at the central of verification and model-checking of both classical and probabilistic systems. Reachability of quantum systems was first studied by physicists [19] within the theme of quantum control , but they only considered states reachable in a single step of evolution. In [24], reachability of qMCs was considered, and it was used in termination checking of concurrent quantum programs. However, reachability studied in [24] can be properly described as *qualitative* reachability because there only algorithms for computing reachable subspaces but not reachability

probabilities were developed. This paper is a continuation of [24] and aims at *quantitative* reachability analysis for qMCs. More precisely, the main purpose of this paper is to develop (classical) algorithms for computing the reachability, repeated reachability and persistence probabilities of qMCs.

Reachability analysis techniques for classical MCs heavily depends on algorithms for graph-reachability problems, in particular for finding bottom strongly connected components (BSCCs) of the underlying graph of a MC (see [2, Section 10.1.2]). Such algorithms have been intensively studied by the graph algorithms community since early 1970's (see [5, Part VI]; [22]), and are ready to be directly adopted in reachability analysis of MCs. However, we don't have the corresponding algorithms for qMCs in hands and have to start from scratch. So, in order to conduct reachability analysis for qMCs we introduce the notion of BSCC and develop an algorithm for finding BSCC decomposition for qMCs in this paper. Interestingly, there are some essential differences between BSCCs in the classical and quantum cases. For example, BSCC decomposition of a qMC is unnecessary to be unique. Also, classical algorithms for finding BSCCs like depth-first search cannot be directly generalised to qMCs. Instead, it requires very different ideas to develop algorithms for finding BSCCS of qMCs, appealing to matrix operation algorithms [5, Chapter 28] through matrix representation of super-operators. The major challenge in dealing with quantum BSCCs, which would not arise in classical BSCCs at all, is to maintain the linear algebraic structure underpinning quantum systems. We believe that these results for quantum BSCCs obtained in this paper are also of independent significance.

This paper is organised as follows. The preliminaries are presented in Sec. 2; in particular we recall the notion of qMC and define the graph structure of a qMC. The notion of BSCC of a qMC is introduced in Sec. 3, where a characterisation of quantum BSCC is given in terms of the fixed points of super-operators, and an algorithm for checking whether a subspace of the state Hilbert space of a QMC is BSCC is given. In Sec. 4, we define the notion of transient subspace of a qMC and show that the state space of a qMC can be decomposed into the direct sum of a transient subspace and a family of BSCCs. Furthermore, it is proved that although such a decomposition is not unique, the dimensions of its components are fixed. In particular, an algorithm for constructing BSCC decomposition of qMCs is found. With the preparation in Secs. 3 and 4, we examine reachability of a qMC in Sec. 5, where an algorithm for computing reachability probability is presented. An algorithm for computing repeated reachability and persistence probabilities is finally developed in Sec. 6. Sec. 7 is a brief conclusion.

2 Quantum Markov Chains and Their Graph Structures

2.1 Basics of Quantum Theory

For convenience of the reader, we recall some basic notions from quantum theory; for details we refer to [17]. The state space of a quantum system is a Hilbert space. In this paper, we only consider a finite-dimensional Hilbert space $\mathcal{H}$, which is just a finite-dimensional complex vector space with inner product. The inner product of two vectors $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ is denoted by $\langle\phi|\psi\rangle$. A pure quantum state is a normalised vector $|\phi\rangle$ in $\mathcal{H}$ with $\langle\phi|\phi\rangle = 1$. We say that two vectors $|\phi\rangle$ and $|\psi\rangle$ are orthogonal, written $|\phi\rangle \perp |\psi\rangle$,

if $\langle\phi|\psi\rangle = 0$. A mixed state is represented by a density operator, i.e. a positive operator ρ on $\mathcal{H}$ with $tr(\rho) = 1$, or equivalently a positive semi-definite and trace-one $n \times n$ matrix if $\dim \mathcal{H} = n$. In particular, for each pure state $|\psi\rangle$, there is a corresponding density operator $\psi = |\psi\rangle\langle\psi|$. For simplicity, we often use pure state $|\psi\rangle$ and density operator ψ interchangeably. A positive operator ρ is called a partial density operator if trace $\mathrm{tr}(\rho) \leq 1$. The set of partial density operators on $\mathcal{H}$ is denoted by $\mathcal{D}(\mathcal{H})$. The support $\mathrm{supp}(\rho)$ of a partial density operator $\rho \in \mathcal{D}(\mathcal{H})$ is defined to be the space spanned by the eigenvectors of ρ with non-zero eigenvalues. The set of all (bounded) operators on $\mathcal{H}$, i.e. $d \times d$ complex matrices with $d = \dim(\mathcal{H})$, is denoted by $\mathcal{B}(\mathcal{H})$.

For any set V of vectors in $\mathcal{H}$, we write $\mathrm{span}V$ for the subspace of $\mathcal{H}$ spanned by V; that is, it consists of all finite linear combinations of vectors in V. Two subspaces X and Y of $\mathcal{H}$ are said to be orthogonal, written $X \perp Y$, if $|\phi\rangle \perp |\psi\rangle$ for any $|\phi\rangle \in X$ and $|\psi\rangle \in Y$. The ortho-complement $X^\perp$ of a subspace X of $\mathcal{H}$ is the subspace of vectors orthogonal to all vectors in X. An operator P is called the projection onto a subspace X if $P|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in X$ and $P|\psi\rangle = 0$ for all $|\psi\rangle \in X^\perp$. We write P_X for the projection onto X. According to the theory of quantum measurements, for any density operator ρ, trace $tr(P_X\rho)$ is the probability that the mixed state ρ lies in subspace X. Let $\{X_k\}$ be a family of subspaces of $\mathcal{H}$. Then the join of $\{X_k\}$ is defined by

$$\bigvee_k X_k = \mathrm{span}(\bigcup_k X_k).$$

In particular, we write $X \vee Y$ for the join of two subspaces X and Y. It is easy to see that $\bigvee_k X_k$ is the smallest subspace of $\mathcal{H}$ that contains all X_k.

Composed quantum systems are modelled by tensor products. If a quantum system consists of two subsystems with state spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, then its state space is $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, which is the Hilbert space spanned by vectors $|\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$. For any operators A_1 on $\mathcal{H}_1$ and A_2 on $\mathcal{H}_2$, their tensor product $A_1 \otimes A_2$ is defined by

$$(A_1 \otimes A_2)(|\psi_1\rangle|\psi_2\rangle) = (A_1|\psi_1\rangle) \otimes (A_2|\psi_2\rangle)$$

for all $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$ together with linearity.

The evolution of a closed quantum system is described as a unitary operator, i.e. an operator U on $\mathcal{H}$ with $U^\dagger U = UU^\dagger = I$, where I is the identity on $\mathcal{H}$. A pure state $|\phi\rangle$ becomes $U|\phi\rangle$ after this unitary evolution U, while a mixed state ρ becomes $U\rho U^\dagger$. The dynamics of an open quantum system is described by a super-operator, i.e. a linear map $\mathcal{E}$ from the space of linear operators on $\mathcal{H}$ into itself, satisfying the following conditions:

1. $\mathrm{tr}[\mathcal{E}(\rho)] \leq \mathrm{tr}(\rho)$ for all $\rho \in \mathcal{D}(\mathcal{H})$, with equality for trace-preserving $\mathcal{E}$;
2. Complete positivity: for any extra Hilbert space $\mathcal{H}_R$, $(\mathcal{I}_R \otimes \mathcal{E})(A)$ is positive provided A is a positive operator on $\mathcal{H}_R \otimes \mathcal{H}$, where $\mathcal{I}_R$ is the identity map on the space of linear operators on $\mathcal{H}_R$.

In this paper, we only consider trace-preserving super-operators. Each super-operator has a Kraus operator-sum representation: $\mathcal{E} = \sum_i E_i \cdot E_i^\dagger$, or more precisely

$$\mathcal{E}(\rho) = \sum E_i \rho E_i^\dagger$$

for all $\rho \in \mathcal{D}(\mathcal{H})$, where E_i are operators on $\mathcal{H}$ such that $\sum_i E^\dagger E_i = I$.

2.2 Quantum Markov Chains

Now we are ready to introduce the notion of quantum Markov chain. Recall that a Markov chain is a pair $\langle S, P\rangle$, where S is a finite set of states, and P is a matrix of transition probabilities, i.e. a mapping $P : S \times S \to [0, 1]$ such that

$$\sum_{t\in S} P(s, t) = 1$$

for every $s \in S$, where $P(s, t)$ is the probability of going from s to t. A quantum Markov chain is a quantum generalisation of a Markov chain where the state space of a Markov chain is replaced by a Hilbert space and its transition matrix is replaced by a super-operator.

Definition 1. *A quantum Markov chain is a pair $\mathcal{G} = \langle \mathcal{H}, \mathcal{E}\rangle$, where $\mathcal{H}$ is a finite-dimensional Hilbert space, and $\mathcal{E}$ is a super-operator on $\mathcal{H}$.*

The behaviour of a quantum Markov chain can be described as follows: if currently the process is in a mixed state ρ, then it will be in state $\mathcal{E}(\rho)$ in the next step. Both ρ and $\mathcal{E}(\rho)$ can be written as statistical ensembles:

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|, \qquad \mathcal{E}(\rho) = \sum_j q_j |\psi_j\rangle\langle\psi_j|,$$

where $p_i, q_j \geq 0$ for all i, j, and $\sum_i p_i = \sum_j q_j = 1$. So, super-operator $\mathcal{E}$ can be understood as an operation that transfers statistical ensemble $\{(p_i, |\phi_i\rangle)\}$ to $\{(q_j, |\psi_j\rangle)\}$. In this way, a quantum Markov chain can be seen as a generalisation of a Markov chain.

2.3 Graphs in Quantum Markov Chains

There is a natural graph structure underlying a quantum Markov chain. This can be seen clearly by introducing adjacency relation in it. To this end, we first introduce an auxiliary notion. The image of a subspace X of $\mathcal{H}$ under a super-operator $\mathcal{E}$ is defined to be

$$\mathcal{E}(X) = \bigvee_{|\psi\rangle\in X} \mathrm{supp}(\mathcal{E}(\psi)).$$

Intuitively, $\mathcal{E}(X)$ is the subspace of $\mathcal{H}$ spanned by the images under $\mathcal{E}$ of states in X.

Definition 2. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain, and let $|\varphi\rangle$ and $|\psi\rangle$ be pure states and ρ and σ mixed states in $\mathcal{H}$. Then*

1. *$|\varphi\rangle$ is adjacent to $|\psi\rangle$ in $\mathcal{G}$, written $|\psi\rangle \to |\varphi\rangle$, if $|\varphi\rangle \in \mathcal{E}(X_\psi)$, where $X_\psi = \mathrm{span}\{|\psi\rangle\}$.*
2. *$|\varphi\rangle$ is adjacent to ρ, written $\rho \to |\varphi\rangle$, if $|\varphi\rangle \in \mathcal{E}(\mathrm{supp}(\rho))$.*
3. *σ is adjacent to ρ, written $\rho \to \sigma$, if $\mathrm{supp}(\sigma) \subseteq \mathcal{E}(\mathrm{supp}(\rho))$.*

Definition 3. *1. A sequence $\pi = \rho_0 \to \rho_1 \to \cdots \to \rho_n$ of adjacent density operators in a quantum Markov chain $\mathcal{G}$ is called a path from ρ_0 to ρ_n in $\mathcal{G}$, and its length is $|\pi| = n$.*

2. For any density operators ρ and σ, if there is a path from ρ to σ then we say that σ is reachable from ρ in $\mathcal{G}$.

Definition 4. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. For any $\rho \in \mathcal{D}(\mathcal{H})$, its reachable space in $\mathcal{G}$ is*

$$\mathcal{R}_{\mathcal{G}}(\rho) = \mathrm{span}\{|\psi\rangle \in \mathcal{H} : |\psi\rangle \text{ is reachable from } \rho \text{ in } \mathcal{G}\}.$$

The following lemma are very useful for our latter discussion.

Lemma 1. *1. (Transitivity of reachability) For any $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, if $\mathrm{supp}(\rho) \subseteq \mathcal{R}_{\mathcal{G}}(\sigma)$, then $\mathcal{R}_{\mathcal{G}}(\rho) \subseteq \mathcal{R}_{\mathcal{G}}(\sigma)$.*

2. [24, Theorem 1] If $d = \dim \mathcal{H}$, then for any $\rho \in \mathcal{D}(\mathcal{H})$, we have

$$\mathcal{R}_{\mathcal{G}}(\rho) = \bigvee_{i=0}^{d-1} \mathrm{supp}(\mathcal{E}^i(\rho)). \tag{1}$$

3 Bottom Strongly Connected Components

3.1 Basic Definitions

The notion of bottom strongly connected component plays an important role in model checking Markov chains. In this section, we extend this notion to the quantum case. We first introduce an auxiliary notation. Let X be a subspace of a Hilbert space, and let $\mathcal{E}$ be a super-operator on $\mathcal{H}$. Then the restriction of $\mathcal{E}$ on X is defined to be super-operator $\mathcal{E}|_X$ with

$$\mathcal{E}|_X(\rho) = P_X \mathcal{E}(\rho) P_X$$

for all $\rho \in \mathcal{D}(X)$, where P_X is the projection onto X.

Definition 5. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. A subspace X of $\mathcal{H}$ is called strongly connected in $\mathcal{G}$ if for any $|\varphi\rangle, |\psi\rangle \in X$, we have $|\varphi\rangle \in \mathcal{R}_{\mathcal{G}_X}(\psi)$ and $|\psi\rangle \in \mathcal{R}_{\mathcal{G}_X}(\varphi)$, where quantum Markov chain $\mathcal{G}_X = \langle X, \mathcal{E}_X \rangle$ is the restriction of $\mathcal{G}$ on X.*

We write $SC(\mathcal{G})$ for the set of strongly connected subspaces of $\mathcal{H}$ in $\mathcal{G}$. It is easy to see that $(SC(\mathcal{G}), \subseteq)$ is an inductive set; that is, for any subset $\{X_i\}$ of $SC(\mathcal{G})$ that is linearly ordered by $\subseteq$, we have $\bigcup_i X_i \in SC(\mathcal{G})$. Thus, by Zorn lemma we assert that there exists a maximal element in $SC(\mathcal{G})$.

Definition 6. *A maximal element of $(SC(\mathcal{G}), \subseteq)$ is called a strongly connected component (SCC) of $\mathcal{G}$.*

To define bottom strongly connected component, we need an auxiliary notion of invariant subspace.

Definition 7. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then a subspace X of $\mathcal{H}$ is said to be invariant in $\mathcal{G}$ if $\mathcal{E}(X) \subseteq X$.*

It is easy to see that if super-operator $\mathcal{E}$ has the Kraus representation $\mathcal{E} = \sum_i E_i \cdot E_i^\dagger$, then X is invariant if and only if $E_i X \subseteq X$ for all i. Recall that in a classical Markov chain, the probability of staying in an invariant subset is non-decreasing. A quantum generalisation of this fact is presented in the following:

Theorem 1. *For any invariant subspace X of $\mathcal{H}$ in a quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$, we have*

$$tr(P_X \mathcal{E}(\rho)) \geq tr(P_X \rho)$$

for all $\rho \in \mathcal{D}(\mathcal{H})$, where P_X is the projection onto X.

Now we are ready to introduce the key notion of this section.

Definition 8. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then a subspace X of $\mathcal{H}$ is called a bottom strongly connected component (BSCC) of $\mathcal{G}$ if it is a SCC of $\mathcal{G}$ and invariant in $\mathcal{G}$.*

Example 1. Consider quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ with state space $\mathcal{H} = \mathrm{span}\{|0\rangle, \cdots, |4\rangle\}$ and super-operator

$$\mathcal{E} = \sum_{i=1}^{5} E_i \cdot E_i^\dagger,$$

where the operators E_i (i=1,...,5) are given as follows:

$$E_1 = \frac{1}{\sqrt{2}}(|1\rangle\langle 0+1| + |3\rangle\langle 2+3|), \quad E_2 = \frac{1}{\sqrt{2}}(|1\rangle\langle 0-1| + |3\rangle\langle 2-3|),$$
$$E_3 = \frac{1}{\sqrt{2}}(|0\rangle\langle 0+1| + |2\rangle\langle 2+3|), \quad E_4 = \frac{1}{\sqrt{2}}(|0\rangle\langle 0-1| + |2\rangle\langle 2-3|),$$
$$E_5 = \frac{1}{10}(|0\rangle\langle 4| + |1\rangle\langle 4| + |2\rangle\langle 4| + 4|3\rangle\langle 4| + 9|4\rangle\langle 4|),$$

and the states used above are defined by

$$|0 \pm 1\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2} \text{ and } |2 \pm 3\rangle = (|2\rangle \pm |3\rangle)/\sqrt{2}.$$

It is easy to see that $B = \mathrm{span}\{|0\rangle, |1\rangle\}$ is a BSCC of quantum Markov chain $\mathcal{G}$, as for any $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in B$, we have $\mathcal{E}(\psi) = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2$.

The following lemma clarifies the relationship between different BSCCs.

Lemma 2. *1. For any two different BSCCs X and Y of quantum Markov chain $\mathcal{G}$, we have $X \cap Y = \{0\}$ (0-dimensional Hilbert space).*

2. If X and Y are two BSCCs of $\mathcal{G}$ with $\dim X \neq \dim Y$, then $X \perp Y$.

3.2 Characterisations of BSCCs

This subsection purports to give two characterisations of BSCCs. The first is presented in terms of reachable space.

Lemma 3. *A subspace X is a BSCC of quantum Markov chain $\mathcal{G}$ if and only if $\mathcal{R}_{\mathcal{G}}(\phi) = X$ for any non-zero $|\phi\rangle \in X$.*

To present the second characterisation, we need the notion of fixed point of super-operator.

Definition 9. *1. A nonzero partial density operator $\rho \in \mathcal{D}(\mathcal{H})$ is called a fixed point state of super-operator $\mathcal{E}$ if $\mathcal{E}(\rho) = \rho$.*

2. A fixed point state ρ of super-operator $\mathcal{E}$ is called minimal if for any fixed point state σ of $\mathcal{E}$, it holds that $supp(\sigma) \subseteq supp(\rho)$ implies $\sigma = \rho$.

The second characterisation of BSCCs establishes a connection between BSCCs and minimal fixed point states.

Theorem 2. *A subspace X is a BSCC of quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ if and only if there exists a minimal fixed point state ρ of $\mathcal{E}$ such that $supp(\rho) = X$. Furthermore, ρ is actually the* unique *fixed point state, up to normalisation, with the support included in X.*

3.3 Checking BSCCs

We now present an algorithm that decides whether or not a given subspace is a BSCC of a quantum Markov chain (see Algorithm 1). The correctness and complexity of this algorithm are given in the following theorem.

Theorem 3. *Give a quantum graph $\langle \mathcal{H}, \mathcal{E} \rangle$ and a subspace $X \subseteq \mathcal{H}$, Algorithm 1 decides whether or not X is a BSCC of $\mathcal{G}$ in time $O(n^6)$, where $n = \dim(\mathcal{H})$.*

4 Decomposition of the State Space

A state in a classical Markov chain is transient if there is a non-zero probability that the process will never return to it, and a state is recurrent if from it the returning probability is 1. It is well-known that a state is recurrent if and only if it belongs to some BSCC in a finite-state Markov chain, and thus the state space of a classical Markov chain can be decomposed into the union of some BSCCs and a transient subspace [2], [16]. The aim of this section is to prove a quantum generalisation of this result.

Definition 10. *A subspace $X \subseteq \mathcal{H}$ is transient in a quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ if*

$$\lim_{k \to \infty} \mathrm{tr}(P_X \mathcal{E}^k(\rho)) = 0$$

for any $\rho \in \mathcal{D}(\mathcal{H})$, where P_X is the projection onto X.

Algorithm 1: CheckBSCC(X)

input : A quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ and a subspace $X \subseteq \mathcal{H}$
output: True or False indicating whether X is a BSCC of $\mathcal{G}$
begin
  if $\mathcal{E}(X) \not\subseteq X$ **then**
    return *False*;
  end
  $\mathcal{E}' \leftarrow P_X \circ \mathcal{E}$;
  $\mathcal{B} \leftarrow$ a density operator basis of the set $\{A \in \mathcal{B}(\mathcal{H}) : \mathcal{E}'(A) = A\}$; (*)
  if $|\mathcal{B}| > 1$ **then**
    return *False*;
  else
    $\rho \leftarrow$ the unique element in $\mathcal{B}$;
    if $X = \mathrm{supp}(\rho)$ **then**
      return *True*;
    else
      return *False*;
    end
  end
end

The above definition is stated in a "double negation" way. Intuitively, it means that the probability in a transient subspace will be eventually zero. To understand this definition better, let us recall that in a classical Markov chain, a state s is said to be transient if the system starting from s will eventually return to s with probability less than 1. It is well-known that in a finite-state Markov chain, this is equivalent to that the probability at this state will eventually become 0. In the quantum case, the property "eventually return" can be hardly described without measurements, and measurements will disturb the behaviours of the systems. So, we choose to adopt the above definition.

To give a characterisation of transient subspace, we need the notion of the asymptotic average of a super-operator $\mathcal{E}$, which is defined to be

$$\mathcal{E}_\infty = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}^n. \tag{2}$$

It is easy to see from [21, Proposition 6.3, Proposition 6.9] that $\mathcal{E}_\infty$ is a super-operator as well.

Theorem 4. *The ortho-complement of the image of the state space $\mathcal{H}$ of a quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ under the asymptotic average of super-operator $\mathcal{E}$:*

$$T_{\mathcal{E}} := \mathcal{E}_\infty(\mathcal{H})^\perp$$

is the largest transient subspace in $\mathcal{G}$; that is, any transient subspace of $\mathcal{G}$ is a subspace of $T_{\mathcal{E}}$.

We now turn to examine the structure of the image of the state space $\mathcal{H}$ under super-operator $\mathcal{E}$.

Theorem 5. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then $\mathcal{E}_\infty(\mathcal{H})$ can be decomposed into the direct sum of some orthogonal BSCCs of $\mathcal{G}$.*

Combining Theorems 4 and 5, we see that the state space of a quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ can be decomposed into the direct sum of a transient subspace of a family of BSCCs:

$$\mathcal{H} = B_1 \oplus \cdots \oplus B_u \oplus T_{\mathcal{E}} \tag{3}$$

where B_i's are orthogonal BSCCs of $\mathcal{G}$. A similar decomposition was recently obtained in [18] for a special case of $\mathcal{E}^2 = \mathcal{E}$. The above decomposition holds for any super-operator $\mathcal{E}$ and thus considerably generalises the corresponding result in [18].

The BSCC and transient subspace decomposition of a classical Markov chain is unique. However, it is not the case for quantum Markov chains; a trivial example is that $\mathcal{E}$ is the identity operator, for which any 1-dimensional subspace of $\mathcal{H}$ is a BSCC, and thus for each othonormal basis $\{|i\rangle\}$ of $\mathcal{H}$, $\bigoplus_i \mathrm{span}\{|i\rangle\}$ is an orthogonal decomposition of $\mathcal{H}$. The following is a more interesting example.

Example 2. Let quantum Markov chain $\mathcal{G} = \langle \mathcal{E}, \mathcal{H} \rangle$ be given as in Example 1. Then $B_1 = \mathrm{span}\{|0\rangle, |1\rangle\}$, $B_2 = \mathrm{span}\{|2\rangle, |3\rangle\}$, $D_1 = \mathrm{span}\{|0+2\rangle, |1+3\rangle\}$, and $D_2 = \mathrm{span}\{|0-2\rangle, |1-3\rangle\}$ are BSCCs, and $T_{\mathcal{E}} = \mathrm{span}\{|4\rangle\}$ is a transient subspace. Furthermore, we have

$$\mathcal{H} = B_1 \oplus B_2 \oplus T_{\mathcal{E}} = D_1 \oplus D_2 \oplus T_{\mathcal{E}}.$$

The relation between different decompositions of a quantum Markov chain is clarified by the following.

Theorem 6. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, and let*

$$\mathcal{H} = B_1 \oplus \cdots \oplus B_u \oplus T_{\mathcal{E}} = D_1 \oplus \cdots \oplus D_v \oplus T_{\mathcal{E}}$$

be two decompositions in the form of Eq. (3), and B_is and D_is are arranged, respectively, according to the increasing order of the dimensions. Then $u = v$, and $\dim(B_i) = \dim(D_i)$ for each $1 \leq i \leq u$.

To conclude this section, we present an algorithm for finding a BSCC and transient subspace decomposition of a quantum Markov chain (see Algorithm 2).

Theorem 7. *Give a quantum graph $\langle \mathcal{H}, \mathcal{E} \rangle$, Algorithm 2 decomposes the Hilbert space $\mathcal{H}$ into the direct sum of a family of orthogonal BSCCs and a transient subspace of $\mathcal{G}$ in time $O(n^8)$, where $n = \dim(\mathcal{H})$.*

5 Reachability Probability

The traditional way to define reachability probabilities in classical Markov chains is first introducing a probability measure based on cylinder sets of finite paths of states. The

Algorithm 2: Decompose($\mathcal{G}$)

input : A quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$
output: A set of orthogonal BSCCs $\{B_i\}$ and a transient subspace $T_{\mathcal{E}}$ such that $\mathcal{H} = \bigoplus_i B_i \oplus T_{\mathcal{E}}$
begin
  $\mathcal{B} \leftarrow$ Decompose($\mathcal{E}_\infty(\mathcal{H})$);
  return $\mathcal{B}$, $\mathcal{E}_\infty(\mathcal{H})^\perp$;
end

probability of reaching a set T is then the probability measure of the set of paths which include a state from T. Typically, reachability probabilities can be obtained by solving a system of linear equations, which is easy and numerically efficient. In quantum Markov chains, however, it is even not clear how to define such a probability measure. Thus it seems hopeless to extend reachability analysis to the quantum case in this way.

Fortunately, there is another way to compute the reachability probability in a classical Markov chain $\langle S, P \rangle$. Given a set of states $T \subseteq S$, we first change the original Markov chain into a new one $\langle S, P' \rangle$ by making states in T absorbing. Then the reachability probability of T is simply the limit of the probability accumulated in T, when the time goes to infinity. It turns out that this equivalent definition can be extended into the quantum case as follows.

Definition 11. *Let $\langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $\rho \in \mathcal{D}(\mathcal{H})$ an initial state, and $G \subseteq \mathcal{H}$ a subspace. Then the probability of reaching G, starting from ρ, can be defined as*

$$\Pr(\rho \vDash \Diamond G) = \lim_{i \to \infty} \mathrm{tr}(P_G \widetilde{\mathcal{E}}^i(\rho))$$

where $\widetilde{\mathcal{E}} = P_G + \mathcal{E} \circ (I - P_G)$ is the super-operator which first performs the projective measurement $\{P_G, I - P_G\}$ and then applies the identity operator $\mathcal{I}$ or $\mathcal{E}$ depending on the measurement outcome.

Obviously the limit in the above definition exists, as the probabilities $\mathrm{tr}(P_G \widetilde{\mathcal{E}}^i(\rho))$ are nondecreasing in i.

To compute the reachability probability, we first note the subspace G is invariant under $\widetilde{\mathcal{E}}$. Thus $\langle G, \widetilde{\mathcal{E}} \rangle$ is again a quantum Markov chain. Since $\widetilde{\mathcal{E}}(I_G) = I_G$ and $\widetilde{\mathcal{E}}_\infty(G) = G$, we can decompose G into a set of orthogonal BSCCs according to $\widetilde{\mathcal{E}}$ by Theorem 5. The following lemma shows a connection between the limit probability of hitting a BSCC and the probability that the asymptotic average of the initial state lies in the same BSCC.

Lemma 4. *Let $\{B_i\}$ be a BSCC decomposition of $\mathcal{E}_\infty(\mathcal{H})$, and P_{B_i} the projection onto B_i. Then for each i, we have*

$$\lim_{k \to \infty} \mathrm{tr}(P_{B_i} \mathcal{E}^k(\rho)) = \mathrm{tr}(P_{B_i} \mathcal{E}_\infty(\rho)) \tag{4}$$

for all $\rho \in \mathcal{D}(\mathcal{H})$.

Procedure Decompose(X)

input : A subspace X which is the support of a fixed point state of $\mathcal{E}$
output: A set of orthogonal BSCCs $\{B_i\}$ such that $X = \oplus B_i$
begin
  $\mathcal{E}' \leftarrow P_X \circ \mathcal{E}$;
  $\mathcal{B} \leftarrow$ a density operator basis of the set $\{A \in \mathcal{B}(\mathcal{H}) : \mathcal{E}'(A) = A\}$;
  if $|\mathcal{B}| = 1$ **then**
    $\rho \leftarrow$ the unique element of $\mathcal{B}$;
    return $\{\mathrm{supp}(\rho)\}$;
  else
    $\rho_1, \rho_2 \leftarrow$ two arbitrary elements of $\mathcal{B}$;
    $\rho \leftarrow$ positive part of $\rho_1 - \rho_2$;
    $Y \leftarrow \mathrm{supp}(\rho)^{\perp}$; (* the ortho-complement of $\mathrm{supp}(\rho)$ in X*)
    return $\mathrm{Decompose}(\mathrm{supp}(\rho)) \cup \mathrm{Decompose}(Y)$;
  end
end

Lemma 4 and Theorem 4 together give us an efficient way to compute the reachability probability from a quantum state to a subspace.

Theorem 8. *Let $\langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $\rho \in \mathcal{D}(\mathcal{H})$, and $G \subseteq \mathcal{H}$ a subspace. Then*

$$\Pr(\rho \vDash \Diamond G) = \mathrm{tr}(P_G \widetilde{\mathcal{E}}_\infty(\rho)),$$

and this probability can be computed in time $O(n^8)$ where $n = \dim(\mathcal{H})$.

Our next results assert that if a quantum Markov chain starts from a pure state in a BSCC then its evolution sequence $\psi, \mathcal{E}(\psi), \mathcal{E}^2(\psi), \cdots$ will hit a subspace with non-zero probability infinitely often provided X is not orthogonal to that BSCC. They establishes indeed a certain fairness and thus can be seen as quantum generalisations of Theorems 10.25 and 10.27 in [2]. It is well-known that in the quantum world a measurement will change the state of the measured system. Consequently, fairness naturally splits into two different versions in quantum Markov chains.

Lemma 5. *(Measure-once fairness) Let B be a BSCC of quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$, and X a subspace which is not orthogonal to B. Then for any $|\psi\rangle \in B$, it holds that $\mathrm{tr}(P_X \mathcal{E}^i(\psi)) > 0$ for infinitely many i.*

Lemma 6. *(Measure-many fairness) Let B be a BSCC of a quantum Markov chain $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$, and $X \subseteq B$ a subspace of B. Then for any $|\psi\rangle \in B$, we have*

$$\lim_{i \to \infty} \mathrm{tr}(\widetilde{\mathcal{E}}^i(\psi)) = 0,$$

where $\widetilde{\mathcal{E}} = P_{X^\perp} \circ \mathcal{E}$, and $X^\perp$ is the ortho-complement of X in $\mathcal{H}$.

Lemma 6 was stated also in a "double negation" way. To best understand it, let us assume that at each step after $\mathcal{E}$ is applied, we perform a projective measurement

$\{P_X, P_{X^\perp}\}$. If the outcome corresponding to P_X is observed, the process terminates immediately; otherwise, it continues with another round of applying $\mathcal{E}$. Lemma 6 asserts that the probability of nontermination is asymptotically 0; in other words, if we set X as an absorbing boundary, which is included in BSCC B, the reachability probability will be absorbed eventually. This lemma is indeed a strong version of fairness. Furthermore, we have:

Theorem 9. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, and let X be a subspace of $\mathcal{H}$, and $\widetilde{\mathcal{E}} = P_{X^\perp} \circ \mathcal{E}$. Then the following two statements are equivalent:*

1. *The subspace $X^\perp$ contains no BSCC;*
2. *For any $\rho \in \mathcal{D}(\mathcal{H})$, we have*

$$\lim_{i \to \infty} \mathrm{tr}(\widetilde{\mathcal{E}}^i(\rho)) = 0.$$

It is worthy noting that in Theorem 9, X is not required to be a subspace of a BSCC B. The following two examples give some simple applications of Theorem 9.

Example 3. Consider a quantum walk on an n-size cycle [1]. The state space of the whole system is $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$, where $\mathcal{H}_p = \mathrm{span}\{|0\rangle, \cdots, |n-1\rangle\}$ is the position space, and $\mathcal{H}_c = \mathrm{span}\{|0\rangle, |1\rangle\}$ is the coin space. The evolution of the systems is described by a unitary transformation $U = S(I \otimes H)$, where the coin operator H is the Hadamard operator, and the shift operator

$$S = \sum_{i=0}^{n-1} (|i+1\rangle\langle i| \otimes |0\rangle\langle 0| + |i-1\rangle\langle i| \otimes |1\rangle\langle 1|)$$

where the arithmetic operations over the index set are understood as modulo n. If we set absorbing boundaries at position 0, then from any initial state $|\psi\rangle$, we know from Theorem 9 that the probability of nontermination is asymptotically 0 because there is no BSCC which is orthogonal to the absorbing boundaries.

Example 4. Consider the quantum Markov chain in Example 1. Let ρ_0 be the initial state, and assume that projective measurement $\{P_0 = |0\rangle\langle 0|, P_1 = I - P_0\}$ will be per formed at the end of each step and P_0 is set as the absorbing boundary. We write $\tilde{\rho}_k = \tilde{\mathcal{E}}^k(\rho_0)$ for the partial density operator after k steps, where $\tilde{\mathcal{E}} = P_1 \circ \mathcal{E}$.

1. If $\rho_0 = |1\rangle\langle 1|$, then $\lim_{k\to\infty} \tilde{\rho}_k = 0$. This means the probability will be eventually absorbed.
2. If $\rho_0 = |2\rangle\langle 2|$, then $\lim_{k\to\infty} \tilde{\rho}_k = (|2\rangle\langle 2| + |3\rangle\langle 3|)/2$. No probability is absorbed. Let D_1 and D_2 be as in Example 2. Then the probabilities in D_1 and D_2 are both 0.5. This means that if $\mathrm{supp}(P_0)$ is not orthogonal to a BSCC D, then the probability in D may not be absorbed.

6 Repeated Reachability and Persistence Probabilities

In this section, we consider how to compute two kinds of reachability probabilities, namely "repeated reachability" and "persistence property", in a quantum Markov chain. Note that $\mathcal{E}_\infty(\mathcal{H})^\perp$ is a transient subspace. We can focus our attention on $\mathcal{E}_\infty(\mathcal{H})$.

Definition 12. *Let $\mathcal{G} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain and G a subspace of $\mathcal{E}_\infty(\mathcal{H})$.*

1. *The set of states in $\mathcal{E}_\infty(\mathcal{H})$ satisfying the repeated reachability* "infinitely often *reaching G" is*

$$\mathcal{X}(G) = \{|\psi\rangle \in \mathcal{E}_\infty(\mathcal{H}) : \lim_{k\to\infty} \mathrm{tr}((P_{G^\perp} \circ \mathcal{E})^k(\psi)) = 0\}.$$

2. *The set of states in $\mathcal{E}_\infty(\mathcal{H})$ satisfying the persistence property* "eventually always *in X" is*

$$\mathcal{Y}(G) = \{|\psi\rangle \in \mathcal{E}_\infty(\mathcal{H}) : (\exists N \geq 0)(\forall k \geq N)\, \mathrm{supp}(\mathcal{E}^k(\psi)) \subseteq G\}.$$

The set $\mathcal{X}(G)$ is defined again in a "double negation" way. Its intuitive meaning can be understood as follows: if the process starts in a state in $\mathcal{X}(G)$ and we make G absorbing, then the probability will be eventually absorbed by G.

The following theorem gives a characterisation of $\mathcal{X}(G)$ and $\mathcal{Y}(G)$ and also clarifies the relationship between them.

Theorem 10. *For any subspace G of $\mathcal{E}_\infty(\mathcal{H})$, both $\mathcal{X}(G)$ and $\mathcal{Y}(G)$ are subspaces of $\mathcal{H}$. Furthermore, we have*

$$\mathcal{X}(G) = \mathcal{E}_\infty(G), \qquad \mathcal{Y}(G) = \bigvee_{B \subseteq G} B = \mathcal{X}(G^\perp)^\perp,$$

where B ranges over all BSCCs, and the orthogonal complements are taken in $\mathcal{E}_\infty(\mathcal{H})$. Moreover, both $\mathcal{X}(G)$ and $\mathcal{Y}(G)$ are invariant.

Example 5. Let us revisit Example 1 where $\mathcal{E}_\infty(\mathcal{H}) = \mathrm{span}\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$.

1. If $G = \mathrm{span}\{|0\rangle, |1\rangle, |2\rangle\}$, then $\mathcal{E}_\infty(G^\perp) = \mathrm{supp}(\mathcal{E}_\infty(|3\rangle\langle 3|)) = \mathrm{supp}((|2\rangle\langle 2| + |3\rangle\langle 3|)/2)$ and $\mathcal{E}_\infty(G) = \mathcal{E}_\infty(\mathcal{H})$. Thus $\mathcal{Y}(G) = B_1$ and $\mathcal{X}(G) = \mathcal{E}_\infty(\mathcal{H})$.
2. If $G = \mathrm{span}\{|3\rangle\}$, then $\mathcal{E}_\infty(G^\perp) = B_1 \oplus B_2$ and $\mathcal{E}_\infty(G) = B_2$. Thus $\mathcal{Y}(G) = \{0\}$ and $\mathcal{X}(G) = B_2$.

Now we can define probabilistic persistence and probabilistic repeated reachability.

Definition 13. *1. The probability that a state ρ satisfies the repeated reachability rep(G) is the eventual probability in $\mathcal{X}(G)$, starting from ρ:*

$$\Pr(\rho \vDash \textit{rep}(G)) = \lim_{k\to\infty} \mathrm{tr}(P_{\mathcal{X}(G)}\mathcal{E}^k(\rho)).$$

2. *The probability that a state ρ satisfies the persistence property pers(G) is the eventual probability in $\mathcal{Y}(G)$, starting from ρ:*

$$\Pr(\rho \vDash \textit{pers}(G)) = \lim_{k\to\infty} \mathrm{tr}(P_{\mathcal{Y}(G)}\mathcal{E}^k(\rho)).$$

The well-definedness of the above definition comes from the fact that $\mathcal{X}(G)$ and $\mathcal{Y}(G)$ are invariant. By Theorem 1 we know that the two sequences $\{\mathrm{tr}(P_{\mathcal{X}(G)}\mathcal{E}^k(\rho))\}$ and $\{\mathrm{tr}(P_{\mathcal{Y}(G)}\mathcal{E}^k(\rho))\}$ are non-decreasing, and thus their limits exist. Combining Theorems 4 and 10, we have:

Theorem 11. *1. The repeated reachability probability is*

$$\Pr(\rho \vDash \mathit{rep}(G)) = 1 - \mathrm{tr}(P_{\mathcal{X}(G)^\perp}\mathcal{E}_\infty(\rho)) = 1 - \Pr(\rho \vDash \mathit{pers}(G^\perp)).$$

2. The persistence probability is

$$\Pr(\rho \vDash \mathit{pers}(G)) = \mathrm{tr}(P_{\mathcal{Y}(G)}\mathcal{E}_\infty(\rho)).$$

Finally, we are able to give an algorithm for computing reachability and persistence probabilities (see Algorithm 3).

Algorithm 3: Persistence(G, ρ)

input : A quantum Markov chain $\langle \mathcal{H}, \mathcal{E}\rangle$, a subspace $G \subseteq \mathcal{H}$, and an initial state $\rho \in \mathcal{D}(\mathcal{H})$

output: The probability $\Pr(\rho \vDash \mathrm{pers}(G))$

begin

$\rho_\infty \leftarrow \mathcal{E}_\infty(\rho)$;

$Y \leftarrow \mathcal{E}_\infty(G^\perp)$;

$P \leftarrow$ the projection onto $Y^\perp$; (* $Y^\perp$ is the ortho-complement of Y in $\mathcal{E}_\infty(\mathcal{H})$ *)

return $\mathrm{tr}(P\rho_\infty)$;

end

Theorem 12. *Give a quantum Markov chain $\langle \mathcal{H}, \mathcal{E}\rangle$, an initial state $\rho \in \mathcal{D}(\mathcal{H})$, and a subspace $G \subseteq \mathcal{H}$, Algorithm 3 computes persistence probability $\Pr(\rho \vDash \mathit{pers}(G))$ in time $O(n^8)$, where $n = \dim(\mathcal{H})$.*

With Theorem 11, Algorithm 3 can also be used to compute repeated reachability probability $\Pr(\rho \vDash \mathrm{rep}(G))$.

7 Conclusions

We introduced the notion of bottom strongly connected component (BSCC) of a quantum Markov chain (qMC) and studied the BSCC decomposition of qMCs. This enables us to develop an efficient algorithm for computing repeated reachability and persistence probabilities of qMCs. Such an algorithm may be used to verify safety and liveness properties of physical systems produced in quantum engineering and quantum programs for future quantum computers.

References

1. A. Ambainis, Quantum walks and their algorithmic applications, *International Journal of Quantum Information*, 1(2003), 507-518.
2. C. Baier and J. -P. Katoen, *Principles of Model Checking*, MIT Press, Cambridge, Massachusetts, 2008.
3. D. Burgarth, G. Chiribella, V. Giovannetti, P. Perinotti and K. Yuasa, Ergodic and Mixing Quantum Channels in Finite Dimensions, *arXiv:1210.5625v1*.
4. J. I. Cirac and P. Zoller, Goals and opportunities in quantum simulation, *Nature Physics*, 8(2012)264-266.
5. T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to Algorithms*, The MIT Press, Cambridge, Massachusetts, 2009.
6. T. A. S. Davidson, *Formal Verification Techniques using Quantum Process Calculus*, Ph.D. thesis, University of Warwick, 2011.
7. E. D'Hondt and P. Panangaden, Quantum weakest preconditions, *Mathematical Structures in Computer Science*, 16(2006)429-451.
8. Y. Feng, R. Y. Duan and M. S. Ying, Bisimulation for quantum processes, *Proceedings of the 38th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, 2011, pp. 523-534.
9. Y. Feng, R. Y. Duan and M. S. Ying, Bisimulation for quantum processes, *ACM Transactions on Programming Languages and Systems*, 34(2012) art. no: 17.
10. C. W. Gardiner and P. Zoller, *Quantum Noise: A Handbook of Markovian and Non-Markovian Stochastic Methods with Applications to Quantum Optics*, Springer, Berlin, 2004.
11. S. J. Gay and R. Nagarajan, Communicating Quantum Processes, *Proceedings of the 32nd ACM Symposium on Principles of Programming Languages (POPL)*, 2005, pp. 145-157.
12. S. J. Gay, N. Papanikolaou and R. Nagarajan, Specification and verification of quantum protocols, *Semantic Techniques in Quantum Computation* (S. J. Gay and I. Mackie, eds.), Cambridge University Press, 2010, pp. 414-472.
13. S. J. Gay, N. Papanikolaou and R. Nagarajan, QMC: a model checker for quantum systems. *Proceedings of the 20th International Conference on Computer Aided Verification (CAV)*, 2008, Springer LNCS 5123, pp. 543-547.
14. S. Hart, M. Sharir and A. Pnueli, Termination of probabilistic concurrent programs, *ACM Transactions on Programming Languages and Systems*, 5(1983)356380.
15. P. Jorrand and M. Lalire, Toward a quantum process algebra, *Proceedings of the First ACM Conference on Computing Frontiers*, 2004, pp. 111-119.
16. M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomised Algorithms and Probabilistic Analysis*, Cambridge University Press, Cambridge, 2005.
17. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
18. A. Rosmanis, Fixed space of positive trace-preserving super-operators, *Linear Algebra and its Applications*, 437(2012), 1704-1721.
19. S. G. Schirmer, A. I. Solomon and J. V. Leahy, Criteria for reachability of quantum states, *Journal of Physics A: Mathematical and General*, 35 (2002), 8551-8562.
20. P. Selinger, Towards a quantum programming language, *Mathematical Structure in Computer Science* 14(2004)527-586.
21. M. M. Wolf, *Quantum Channels and Operators: Guided Tour*, unpublished.
22. M. Yannakakis, Graph-theoretic methods in database theory, in: *Proc. of the 9th ACM Symposium on Principles of Database Systems*, 1990, pp. 230-242.
23. M. S. Ying, Floyd-Hoare logic for quantum programs, *ACM Transactions on Programming Languages and Systems*, 33(2011) art. no: 19.

24. N. K. Yu and M. S. Ying, Reachability and termination analysis of quantum concurrent programs, in: *Proc. of CONCUR 2012*, LNCS 7455, Springer, pp. 69-83.
25. M. S. Ying, N. K. Yu, Y. Feng and R. Y. Duan, Verification of Quantum Programs, *Science of Computer Programming* (accepted, 2013) (also see: *arXiv:1106.4063*).

A Proofs of Lemmas and Theorems

We first collect some simple properties of the support of super-operators for our latter use.

Proposition 1. *1. If $A = \sum_k \lambda_k |\phi_k\rangle\langle\phi_k|$ where all $\lambda_k > 0$ (but $|\phi_k\rangle$'s are not required to be pairwise orthogonal), then* $\mathrm{supp}(A) = \mathrm{span}\{|\phi_k\rangle\}$;
2. $\mathrm{supp}(\mathcal{E}(\rho+\sigma)) = \mathrm{supp}(\mathcal{E}(\rho)) \vee \mathrm{supp}(\mathcal{E}(\sigma))$;
3. If $\mathcal{E} = \sum_{i\in I} E_i \cdot E_i^\dagger$, then $\mathcal{E}(X) = \mathrm{span}\{E_i|\psi\rangle : i \in I, |\psi\rangle \in X\}$;
4. $\mathcal{E}(X_1 \vee X_2) = \mathcal{E}(X_1) \vee \mathcal{E}(X_2)$. Thus, $X \subseteq Y \Rightarrow \mathcal{E}(X) \subseteq \mathcal{E}(Y)$.

Let $\mathcal{E} = \sum_i E_i \cdot E_i^\dagger$ be a super-operator on an n-dimensional Hilbert space $\mathcal{H}$. The matrix representation M of $\mathcal{E}$ is an $n^2 \times n^2$ matrix $M = \sum_i E_i \otimes E_i^*$ [25,21]. Let $M = SJS^{-1}$ be the Jordan decomposition of M where

$$J = \bigoplus_{k=1}^{K} J_k(\lambda_k),$$

and $J_k(\lambda_k)$ is a Jordan block corresponding to the eigenvalue λ_k. Define

$$J_\infty = \bigoplus_{k:\lambda_k=1} J_k(\lambda_k)$$

and $M_\infty = SJ_\infty S^{-1}$. Then from [21, Proposition 6.3], we know that M_∞ is exactly the matrix representation of $\mathcal{E}_\infty$.

Lemma 7. *Let $\langle \mathcal{H}, \mathcal{E}\rangle$ be a quantum Markov chain with* $\dim(\mathcal{H}) = n$*, and $\rho \in \mathcal{D}(\mathcal{H})$.*

1. *The asymptotic average of ρ under $\mathcal{E}$, i.e. $\mathcal{E}_\infty(\rho)$, can be computed in time $O(n^8)$.*
2. *A density operator basis of the set $\{A \in \mathcal{B}(\mathcal{H}) : \mathcal{E}(A) = A\}$ can be computed in time $O(n^6)$.*

Proof. 1. Note that the time complexity of Jordan decomposition is $O(d^4)$ for a $d \times d$ matrix. We can compute M_∞, the matrix representation of $\mathcal{E}_\infty$, in time $O(n^8)$. Then $\mathcal{E}_\infty(\rho)$ can be easily derived from the correspondence

$$(\mathcal{E}_\infty(\rho) \otimes I_\mathcal{H})|\Psi\rangle = M_\infty(\rho \otimes I_\mathcal{H})|\Psi\rangle$$

where $|\Psi\rangle = \sum_{i=1}^n |i\rangle|i\rangle$ is the (unnormalised) maximally entangled state in $\mathcal{H}\otimes\mathcal{H}$.

2. We compute the density operator basis by the following three steps:
   (i) Compute the matrix representation M of $\mathcal{E}$. The time complexity is $O(mn^4)$, where $m \leq n^2$ is the number of E_i's in $\mathcal{E} = \sum_i E_i \cdot E_i^\dagger$.
   (ii) Find a basis $\mathcal{B}$ for the null space of the matrix $M - I_{\mathcal{H}\otimes\mathcal{H}}$, and transform them into matrix forms. This can be done by Guassian elimination with complexity being $O((n^2)^3) = O(n^6)$.

(iii) For each basis matrix A in $\mathcal{B}$, compute positive matrices X_+, X_-, Y_+, Y_- such that $\mathrm{supp}(X_+) \perp \mathrm{supp}(X_-)$, $\mathrm{supp}(Y_+) \perp \mathrm{supp}(Y_-)$, and $A = X_+ - X_- + i(Y_+ - Y_-)$. Let Q be the set of nonzero elements in $\{X_+, X_-, Y_+, Y_-\}$. Then by [21, Proposition 6.8], every element of Q is a fixed point state of $\mathcal{E}$. Replace A by elements of Q after normalisation. Then the resultant $\mathcal{B}$ is the required density operator basis. At last, we make the elements in $\mathcal{B}$ linearly independent. This can be done by removing elements in $\mathcal{B}$ using Guassian elimination. The computational complexity of this step is $O(n^6)$.

With these steps, we know the total complexity is $O(n^6)$. □

Proof of Lemma 1. We only prove part 1; for the proof of part 2, see [24]. It follows from

$$\mathrm{supp}(\rho) \subseteq \mathcal{R}_{\mathcal{G}}(\sigma) = \bigvee_{n=0}^{\infty} \mathrm{supp}(\mathcal{E}^n(\sigma))$$

that

$$\begin{aligned}\mathcal{R}_{\mathcal{G}}(\rho) = \bigvee_{m=0}^{\infty} \mathcal{E}^m(\mathrm{supp}(\rho)) &\subseteq \bigvee_{m=0}^{\infty} \mathcal{E}^m(\bigvee_{n=0}^{\infty} \mathrm{supp}(\mathcal{E}^n(\sigma))) \\ &= \bigvee_{i=0}^{\infty} \mathrm{supp}(\mathcal{E}^i(\sigma)) = \mathcal{R}_{\mathcal{G}}(\sigma).\end{aligned}$$

□

Proof of Theorem 1. Let $X^\perp$ be the ortho-complement of X and Q the projection onto $X^\perp$. Then $P_X + Q = I$. Let $\mathcal{E}^* = \sum_i E_i^\dagger \cdot E_i$ be the Schrödinger-Heisenberg dual of $\mathcal{E}$. Since X is invariant under $\mathcal{E}$, we have $\langle\psi|E_i|\phi\rangle = 0$ for any $|\phi\rangle \in X$, $|\psi\rangle \in X^\perp$ and for any i. Thus $\mathcal{E}^*(Q)$ is in $X^\perp$. Furthermore, it holds that $\mathcal{E}^*(Q) \leq \mathcal{E}^*(I) = I$. This implies $\mathcal{E}^*(Q) \leq Q$. Finally, we have

$$\begin{aligned}\mathrm{tr}(P_X\mathcal{E}(\rho)) &= \mathrm{tr}(\mathcal{E}^*(P_X)\rho) \\ &= \mathrm{tr}(\mathcal{E}^*(I)\rho) - \mathrm{tr}(\mathcal{E}^*(Q)\rho) \geq \mathrm{tr}(\rho) - \mathrm{tr}(Q\rho) = \mathrm{tr}(P_X\rho).\end{aligned}$$

□

Proof of Lemma 3. We only prove the necessity part; the sufficiency part is obvious. Suppose X is a BSCC. By the strong connectivity of X, we have $\mathcal{R}_{\mathcal{G}}(\psi) \supseteq X$ for all $|\psi\rangle \in X$. On the other hand, we have from the invariance of X that $\mathcal{E}(X) \subseteq X$. Thus $\mathcal{R}_{\mathcal{G}}(\phi) = X$ for any non-zero vector $|\phi\rangle$ in X. □

Proof of Lemma 2. Part 1: Suppose conversely that there exists a nonzero vector $|\phi\rangle \in A \cap B$. Then by Lemma 3, we have $A = \mathcal{R}_{\mathcal{G}}(\phi) = B$, contradicting the assumption that $A \neq B$. Therefore $A \cap B = \{0\}$.

Part 2: We postpone this part after the proof of Theorem 5. □

Before proving Theorem 2, we recall some basic properties of fixed point states. For more details, we refer to [3,21].

Lemma 8. *([21, Proposition 6.3, Proposition 6.9]) If $\mathcal{E}$ is a sper-operator on $\mathcal{H}$, then*

1. *for any density operator ρ, $\mathcal{E}_\infty(\rho)$ is a fixed point state of $\mathcal{E}$;*
2. *for any fixed point state σ, it holds that* $\mathrm{supp}(\sigma) \subseteq \mathcal{E}_\infty(\mathcal{H})$.

An operator (not necessarily a partial density operator) $A \in \mathcal{B}(\mathcal{H})$ is called a fixed point of super-operator $\mathcal{E}$ if $\mathcal{E}(A) = A$

Lemma 9. *Let $\mathcal{E}$ be a super-operator on $\mathcal{H}$. Then*

1. *([21, Proposition 6.8]) If A is a fixed point of $\mathcal{E}$, and*

$$A = (X_+ - X_-) + i(Y_+ - Y_-)$$

   where X_+, X_-, Y_+, Y_- are positive operators with $\mathrm{supp}(X_+) \perp \mathrm{supp}(X_-)$ *and* $\mathrm{supp}(Y_+) \perp \mathrm{supp}(Y_-)$*, then X_+, X_-, Y_+, Y_- are all fixed points of $\mathcal{E}$.*
2. *([3, Lemma 2]) If ρ is a fixed point state for $\mathcal{E}$, then $supp(\rho)$ is an invariant subspace. Conversely, if X is an invariant subspace of $\mathcal{E}$, then there exists a fixed point state ρ_X such that $supp(\rho_X) \subseteq X$.*

Proof of Theorem 2. We first prove the sufficiency part. Let ρ be a minimal fixed point state such that $supp(\rho) = X$. Then by Lemma 9.2, X is an invariant subspace. To show that X is a BSCC, by Lemma 3 it suffices to prove for any $|\phi\rangle \in X$, $\mathcal{R}_\mathcal{G}(\phi) = X$. Suppose conversely there exists $|\psi\rangle \in X$ such that $\mathcal{R}_\mathcal{G}(\psi) \subsetneq X$. Then by Lemma 1 $\mathcal{R}_\mathcal{G}(\psi)$ is an invariant subspace of $\mathcal{E}$ as well. By Lemma 9.2, we can find a fixed point state ρ_ψ with $\mathrm{supp}(\rho_\psi) \subseteq \mathcal{R}_\mathcal{G}(\psi) \subsetneq X$, contradicting the assumption that ρ is minimal.

For the necessity part, let X be a BSCC. Then X is invariant, and by Lemma 9.2, we can find a minimal fixed point state ρ_X with $\mathrm{supp}(\rho_X) \subseteq X$. Take $|\phi\rangle \in \mathrm{supp}(\rho_X)$. By Lemma 2 we have $\mathcal{R}_\mathcal{G}(\phi) = X$. But on the other hand, by Lemma 9.2 again we have $\mathrm{supp}(\rho_X)$ is invariant, so $\mathcal{R}_\mathcal{G}(\phi) \subseteq \mathrm{supp}(\rho_X)$. Thus $\mathrm{supp}(\rho_X) = X$ indeed.

Finally, the uniqueness of ρ comes from the observation that whenever ρ and σ are both fixed point states of $\mathcal{E}$, then so are $\lambda\rho + \gamma\sigma$, provided that it is nonzero, for any real numbers λ and γ. □

Proof of Theorem 3. By Theorem 2, to check whether a subspace X is a BSCC, it is sufficient to check the following two properties:

1. X is invariant;
2. Every fixed point state of $\mathcal{E}|_X$ has X as its support.

That justifies the correctness of Algorithm 1. The complexity of this algorithm mainly comes from the statement $(*)$ which, according to Lemma 7.2, can be computed in time $O(n^6)$. □

Proof of Theorem 4. Let P be the projection onto $T_\mathcal{E}$, $\rho \in \mathcal{D}(\mathcal{H})$, and $p_k = \mathrm{tr}(P\mathcal{E}^k(\rho))$. Since $\mathcal{E}_\infty(\mathcal{H})$ is an invariant subspace, by Theorem 1 we have p_k is nonincreasing.

Thus the limit $p_\infty = \lim_{k\to\infty} p_k$ does exist. Furthermore, noting that $\mathrm{supp}(\mathcal{E}_\infty(\rho)) \subseteq \mathcal{E}_\infty(\mathcal{H})$, we have

$$\begin{aligned} 0 = \mathrm{tr}(P\mathcal{E}_\infty(\rho)) &= \mathrm{tr}\left(P \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \mathcal{E}^n(\rho)\right) \\ &= \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \mathrm{tr}(P\mathcal{E}^n(\rho)) = \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} p_n \\ &\geq \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} p_\infty = p_\infty. \end{aligned}$$

Thus $p_\infty = 0$, and $T_\mathcal{E}$ is transient by the arbitrariness of ρ.

To show that $T_\mathcal{E}$ is the largest transient subspace of $\mathcal{G}$, note that $\mathrm{supp}(\mathcal{E}_\infty(I)) = \mathcal{E}_\infty(\mathcal{H})$. Let $\sigma = \mathcal{E}_\infty(I/d)$. Then by Lemma 8, σ is a fixed point state with $\mathrm{supp}(\sigma) = T_\mathcal{E}^\perp$. Suppose Y is a transient subspace. We have

$$\lim_{i\to\infty} \mathrm{tr}(P_Y \mathcal{E}^i(\sigma)) = \mathrm{tr}(P_Y\sigma) = 0.$$

This implies $Y \perp \mathrm{supp}(\sigma) = T_\mathcal{E}^\perp$. That is $Y \subseteq T_\mathcal{E}$. □

Lemma 10. *Let ρ and σ be two fixed point state of $\mathcal{E}$, and $\mathrm{supp}(\sigma) \subsetneqq \mathrm{supp}(\rho)$. Then there exists another fixed point state η with $\mathrm{supp}(\eta)\perp\mathrm{supp}(\sigma)$ such that*

$$\mathrm{supp}(\rho) = \mathrm{supp}(\eta) \oplus \mathrm{supp}(\sigma).$$

Proof. Note that for any $\lambda > 0$, $\rho - \lambda\sigma$ is again a fixed point of $\mathcal{E}$. We can take λ sufficiently large such that $\rho - \lambda\sigma = \Delta_+ - \Delta_-$ with $\Delta_\pm \geq 0$, $\mathrm{supp}(\Delta_-) = \mathrm{supp}(\sigma)$, and $\mathrm{supp}(\Delta_+)$ is the orthogonal complement of $\mathrm{supp}(\Delta_-)$ in $\mathrm{supp}(\rho)$. By Lemma 9.1, both Δ_+ and Δ_- are again fixed point states of $\mathcal{E}$. Let $\eta = \Delta_+$. We have

$$\mathrm{supp}(\rho) = \mathrm{supp}(\rho - \lambda\sigma) = \mathrm{supp}(\Delta_+) \oplus \mathrm{supp}(\Delta_-) = \mathrm{supp}(\eta) \oplus \mathrm{supp}(\sigma).$$

□

The following corollary is immediately from Lemma 10.

Corollary 1. *Let ρ be a fixed point state of $\mathcal{E}$. Then $\mathrm{supp}(\rho)$ can be decomposed into the direct sum of some orthogonal BSCCs.*

Proof. If ρ is minimal, then by Theorem 2, $\mathrm{supp}(\rho)$ is itself a BSCC and we are done. Otherwise, we apply Lemma 10 to obtain two fixed point states of $\mathcal{E}$ with smaller orthogonal supports. Repeating this procedure, we will get a set of minimal fixed point states $\rho_1, \cdots, \rho_k$ with mutually orthogonal supports, and

$$\mathrm{supp}(\rho) = \bigoplus_{i=1}^{k} \mathrm{supp}(\rho_i).$$

Finally, from Lemma 9.2 and Theorem 2, each $\mathrm{supp}(\rho_i)$ is a BSCC. □

Proof of Theorem 5. Direct from Corollary 1 by noting that $\mathcal{E}_\infty(I)$ is a fixed point state of $\mathcal{E}$ with $\mathrm{supp}(\mathcal{E}_\infty(I)) = \mathcal{E}_\infty(\mathcal{H})$. □

Proof of Lemma 2.2. Suppose without loss of generality that $\dim(B_1) < \dim(B_2)$. Let ρ and σ be the minimal fixed point states corresponding to B_1 and B_2, respectively. Then from Theorem 2, $\mathrm{supp}(\rho) = B_1$ and $\mathrm{supp}(\sigma) = B_2$. Similar to the proof of Lemma 10, we can take λ sufficiently large such that $\rho - \lambda\sigma = \Delta_+ - \Delta_-$ with $\Delta_\pm \geq 0$, $\mathrm{supp}(\Delta_-) = \mathrm{supp}(\sigma)$, and $\mathrm{supp}(\Delta_+) \perp \mathrm{supp}(\Delta_-)$. Let P be the projection onto B_2. Then

$$P\rho P = \lambda P\sigma P + P\Delta_+ P - P\Delta_- P = \lambda\sigma - \Delta_-$$

is a fixed point state as well. Note $\mathrm{supp}(P\rho P) \subseteq B_2$ and the fact that σ is the minimal fixed point state corresponding to B_2. It follows that $P\rho P = p\sigma$ for some $p \geq 0$. Now if $p > 0$, then by Proposition 1.3 we have

$$B_2 = \mathrm{supp}(\sigma) = \mathrm{supp}(P\rho P) = \mathrm{span}\{P|\psi\rangle : |\psi\rangle \in B_1\}.$$

This implies $\dim(B_2) \leq \dim(B_1)$, contradicting our assumption. Thus we have $P\rho P = 0$, which implies $B_1 \perp B_2$. □

Proof of Theorem 6. Let $b_i = \dim(B_i)$, and $d_i = \dim(D_i)$. We prove by induction that $b_i = d_i$ for any $1 \leq i \leq \min\{u, v\}$. Thus $u = v$ as well.

First, we claim $b_1 = d_1$. Otherwise let, say, $b_1 < d_1$. Then $b_1 < d_j$ for any j. Thus by Lemma 2.2, we have

$$B_1 \perp \bigoplus_{j=1}^{v} D_j.$$

But we also have $B_1 \perp T_{\mathcal{E}}$, a contradiction as

$$\bigoplus_{j=1}^{v} D_j \bigoplus T_{\mathcal{E}} = \mathcal{H}.$$

Suppose we have $b_i = d_i$ for any $i < n$. We claim $b_n = d_n$ as well. Otherwise let, say, $b_n < d_n$. Then from Lemma 2.2, we have

$$\bigoplus_{i=1}^{n} B_i \perp \bigoplus_{i=n}^{v} D_i,$$

and hence

$$\bigoplus_{i=1}^{n} B_i \subseteq \bigoplus_{i=1}^{n-1} D_i.$$

On the other hand, we have

$$\dim(\bigoplus_{i=1}^{n} B_i) = \sum_{i=1}^{n} b_i > \sum_{i=1}^{n-1} d_i = \dim(\bigoplus_{i=1}^{n-1} D_i),$$

a contradiction. □

Proof of Theorem 7. The correctness of Algorithm 2 follows from Theorem 4, Lemma 9 and Corollary 1. For the time complexity, note that similar to Algorithm 1, the non-recursive part of the procedure $Decompose(X)$ runs in time $O(n^6)$. Thus its total complexity is $O(n^7)$, as the procedure calls itself at most $O(n)$ times.

Algorithm 2 first computes $\mathcal{E}_\infty(\mathcal{H})$, which costs time $O(n^8)$, by Lemma 7.1, and then feeds it into the procedure $Decompose(X)$. Thus the total complexity of Algorithm 2 is $O(n^8)$. □

Proof of Lemma 4. Let P be the projection onto $T_\mathcal{E} = \mathcal{E}_\infty(\mathcal{H})^\perp$. Similar to the proof of Theorem 4, we have

$$q_i = \lim_{k\to\infty} \mathrm{tr}(P_{B_i}\mathcal{E}^k(\rho))$$

does exist, and $\mathrm{tr}(P_{B_i}\mathcal{E}_\infty(\rho)) \leq q_i$. Moreover

$$1 = \mathrm{tr}((I-P)\mathcal{E}_\infty(\rho)) = \sum_i \mathrm{tr}(P_{B_i}\mathcal{E}_\infty(\rho)) \leq \sum_i q_i = \lim_{k\to\infty} \mathrm{tr}((I-P)\mathcal{E}^k(\rho)) = 1.$$

This implies $q_i = \mathrm{tr}(P_{B_i}\mathcal{E}_\infty(\rho))$. □

Proof of Theorem 8. The claim that

$$\Pr(\rho \vDash \Diamond G) = \mathrm{tr}(P_G\widetilde{\mathcal{E}}_\infty(\rho))$$

is directly from Lemma 4 and Theorem 4, and the time complexity of computing this quantity follows from Lemma 7.1. □

Proof of Lemma 5. As X is not orthogonal to B, we can always find a pure state $|\phi\rangle \in B$ such that $P_X|\phi\rangle \neq 0$. Now for any $|\psi\rangle \in B$, if there exists N such that $\mathrm{tr}(P_X\mathcal{E}^k(\psi)) = 0$ for any $k > N$. Then $|\phi\rangle \notin \mathcal{R}_\mathcal{G}(\mathcal{E}^{N+1}(\psi))$, which means that $\mathcal{R}_\mathcal{G}(\mathcal{E}^{N+1}(\psi))$ is a proper invariant subspace of B. This contradicts the assumption that B is a BSCC. Thus we have $\mathrm{tr}(P_X\mathcal{E}^i(\psi)) > 0$ for infinitely many i. □

Proof of Lemma 6. Similar to Proposition 6.2 in [21] and Lemma 4.1 in [25], we can show that the limit

$$\widetilde{\mathcal{E}}_\infty := \lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \widetilde{\mathcal{E}}^n$$

exists as well. For any $|\psi\rangle \in B$, we claim that $\rho_\psi := \widetilde{\mathcal{E}}_\infty(\psi)$ is a zero operator. Otherwise, it is easy to check that ρ_ψ is a fixed point of $\widetilde{\mathcal{E}}$. Furthermore, from the fact that

$$\mathcal{E}(\rho_\psi) = \widetilde{\mathcal{E}}(\rho_\psi) + P_X\mathcal{E}(\rho_\psi)P_X = \rho_\psi + P_X\mathcal{E}(\rho_\psi)P_X,$$

we have $\mathrm{tr}(P_X\mathcal{E}(\rho_\psi)) = 0$ as $\mathcal{E}$ is trace-preserving. Thus $P_X\mathcal{E}(\rho_\psi) = 0$, and ρ_ψ is also a fixed point of $\mathcal{E}$. Note that $\mathrm{supp}(\rho_\psi) \subseteq X^\perp \cap B$. This contradicts with the assumption that B is a BSCC, by Theorem 2.

With the claim, and the fact that $\mathrm{tr}(\widetilde{\mathcal{E}}^i(\psi))$ is non-increasing in i, we immediately have $\lim_{i\to\infty} \mathrm{tr}(\widetilde{\mathcal{E}}^i(\psi)) = 0$. □

Proof of Theorem 9. Similar to the proof of Lemma 6. □

To prove Theorem 10, we need the following lemma.

Lemma 11. *Suppose $\mathcal{E}_\infty(\mathcal{H})$ has a proper invariant subspace S. Then for any density operator ρ with $\mathrm{supp}(\rho) \subseteq \mathcal{E}_\infty(\mathcal{H})$ and any integer k, we have*

$$\mathrm{tr}(P_S\mathcal{E}^k(\rho)) = \mathrm{tr}(P_S\rho)$$

where P_S is the projection onto S.

Proof. By Lemma 10, there exists an invariant subspace T such that $\mathcal{E}_\infty(\mathcal{H}) = S \oplus T$ where S and T are orthogonal and invariant. Then by Theorem 1, we have

$$1 \geq \mathrm{tr}(P_S\mathcal{E}^k(\rho)) + \mathrm{tr}(P_T\mathcal{E}^k(\rho)) \geq \mathrm{tr}(P_S\rho) + \mathrm{tr}(P_T\rho) = \mathrm{tr}(\rho) = 1.$$

Thus $\mathrm{tr}(P_S\mathcal{E}^k(\rho)) = \mathrm{tr}(P_S\rho)$. □

Proof of Theorem 10. We first show that $\mathcal{Y}(G)$ is a subspace. Let $|\psi_i\rangle \in \mathcal{Y}(G)$ and α_i be complex numbers, $i = 1, 2$. Then there exists N_i such that for any $j \geq N_i$, $\mathrm{supp}(\mathcal{E}^j(\psi_i)) \subseteq G$. Let $|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$ and $\rho = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|$. Then $|\psi\rangle \in \mathrm{supp}(\rho)$, and from Propositions 1.1, 1.2, and 1.4 we have

$$\mathrm{supp}(\mathcal{E}^j(\psi)) \subseteq \mathrm{supp}(\mathcal{E}^j(\rho)) = \mathrm{supp}(\mathcal{E}^j(\psi_1)) \vee \mathrm{supp}(\mathcal{E}^j(\psi_2))$$

for any $j \geq 0$. Now $|\psi\rangle \in \mathcal{Y}(G)$ follows by letting $N = \max\{N_1, N_2\}$.

We divide the rest of proof into six parts.

– Claim 1: $\mathcal{Y}(G) \supseteq \bigvee_{B\subseteq G} B$.

For any BSCC $B \subseteq G$, from Lemmas 8.2 and 9.2 we have $B \subseteq \mathcal{E}_\infty(\mathcal{H})$. Furthermore, as B is a BSCC, for any $|\psi\rangle \in B$ and any i, $\mathrm{supp}(\mathcal{E}^i(\psi)) \subseteq B \subseteq G$. Thus $B \subseteq \mathcal{Y}(G)$, and the result follows from the fact that $\mathcal{Y}(G)$ is a subspace.

– Claim 2: $\mathcal{Y}(G) \subseteq \bigvee_{B\subseteq G} B$.

For any $|\psi\rangle \in \mathcal{Y}(G)$, note that $\rho_\psi := \mathcal{E}_\infty(\psi)$ is a fixed point state. Let $X = \mathrm{supp}(\rho_\psi)$. We claim $|\psi\rangle \in X$. This is obvious if $X = \mathcal{E}_\infty(\mathcal{H})$. Otherwise, as $\mathcal{E}_\infty(I_\mathcal{H})$ is a fixed point state and $\mathcal{E}_\infty(\mathcal{H}) = \mathrm{supp}(\mathcal{E}_\infty(I_\mathcal{H}))$, by Lemma 10 we have $\mathcal{E}_\infty(\mathcal{H}) = X \oplus X^\perp$, where $X^\perp$, the ortho-complement of X in $\mathcal{E}_\infty(\mathcal{H})$, is also invariant. As X is again a direct sum of some orthogonal BSCCs, by Lemma 4 we have

$$\lim_{i\to\infty} \mathrm{tr}(P_X\mathcal{E}^i(\psi)) = \mathrm{tr}(P_X\mathcal{E}_\infty(\psi)) = 1;$$

that is,

$$\lim_{i\to\infty} \mathrm{tr}(P_{X^\perp}\mathcal{E}^i(\psi)) = 0.$$

Together with Theorem 1, this implies $\mathrm{tr}(P_{X^\perp}\psi) = 0$, and so $|\psi\rangle \in X$.

By the definition of $\mathcal{Y}(G)$, there exists $M \geq 0$, such that $\mathrm{supp}(\mathcal{E}^i(\psi)) \subseteq G$ for all $i \geq M$. Thus

$$X = \mathrm{supp}(\lim_{N\to\infty} \frac{1}{N}\sum_{i=1}^{N} \mathcal{E}^i(\psi)) = \mathrm{supp}(\lim_{N\to\infty} \frac{1}{N}\sum_{i=M}^{N} \mathcal{E}^i(\psi)) \subseteq G.$$

Furthermore, since X can be decomposed into the direct sum of some BSCCs, we have $X \subseteq \bigvee_{B\subseteq G} B$. Then the result follows by noting $|\psi\rangle \in X$.

– Claim 3: $\mathcal{Y}(G^\perp)^\perp \subseteq \mathcal{X}(G)$.

First, from Claims 1 and 2 above we have $\mathcal{Y}(G^\perp) \subseteq G^\perp$ and $G' := \mathcal{Y}(G^\perp)^\perp$ is invariant. Thus $G \subseteq \mathcal{Y}(G^\perp)^\perp$, and $\mathcal{E}$ is a also CPTP map on G'; that is, the pair $\langle G', \mathcal{E}\rangle$ is again a quantum graph. Furthermore, Claim 1 implies that any BSCC in $G^\perp$ is also contained in $\mathcal{Y}(G^\perp)$. Thus there is no BSCC in $G' \cap G^\perp$. By Theorem 9, for any $|\psi\rangle \in G'$, $\lim_{i\to\infty} \mathrm{tr}[(P_{G^\perp} \circ \mathcal{E})^i(\psi)] = 0$. Thus $|\psi\rangle \in \mathcal{X}(G)$ by definition.

– Claim 4: $\mathcal{X}(G) \subseteq \mathcal{Y}(G^\perp)^\perp$.

Similar to Claim 3, we have $\mathcal{Y}(G^\perp) \subseteq G^\perp$ and $\mathcal{Y}(G^\perp)$ is invariant. Let P be the projection onto $\mathcal{Y}(G^\perp)$. Then $P_{G^\perp} P P_{G^\perp} = P$. For any $|\psi\rangle \in \mathcal{X}(G)$, we calculate

$$\mathrm{tr}(P(P_{G^\perp} \circ \mathcal{E})(\psi)) = \mathrm{tr}(P_{G^\perp} P P_{G^\perp} \mathcal{E}(\psi)) = \mathrm{tr}(P\mathcal{E}(\psi)) \geq \mathrm{tr}(P\psi),$$

where the last inequality is by Theorem 1. Therefore

$$0 = \lim_{i\to\infty} \mathrm{tr}((P_{G^\perp} \circ \mathcal{E})^i(\psi)) \geq \lim_{i\to\infty} \mathrm{tr}(P(P_{G^\perp} \circ \mathcal{E})^i(\psi)) \geq \mathrm{tr}(P\psi),$$

and so $|\psi\rangle \in \mathcal{Y}(G^\perp)^\perp$.

– Claim 5: $\bigvee_{B\subseteq G} B \subseteq \mathcal{E}_\infty(G^\perp)^\perp$.

Suppose a BSCC $B \subseteq G$. Then we have $\mathrm{tr}(P_B I_{G^\perp}) = 0$, and so $\mathrm{tr}(P_B \mathcal{E}^i(I_{G^\perp})) = 0$ for any $i \geq 0$ by Lemma 11. Thus $\mathrm{tr}(P_B \mathcal{E}_\infty(I_{G^\perp})) = 0$, leading to $B \perp \mathcal{E}_\infty(G^\perp)$. Therefore $B \subseteq \mathcal{E}_\infty(G^\perp)^\perp$. Then the result follows from the fact that $\mathcal{E}_\infty(G^\perp)^\perp$ is a subspace.

– Claim 6: $\mathcal{E}_\infty(G^\perp)^\perp \subseteq \bigvee_{B\subseteq G} B$.

By Corollary 1, $\mathcal{E}_\infty(G^\perp)^\perp$ can be decomposed into direct sum of BSCCs B_i. For any B_i, we have $\mathrm{tr}(P_{B_i} \mathcal{E}_\infty(I_{G^\perp})) = 0$. Thus $\mathrm{tr}(P_{B_i} I_{G^\perp}) = 0$, meaning that $B_i \perp G^\perp$. Therefore $B_i \subseteq G$, and the result holds.

The invariance of $\mathcal{X}(G)$ and $\mathcal{Y}(G)$ is already included in Claims 1 and 2. This complete the proof. □

Proof of Theorem 12. The correctness of Algorithm 3 follows from Theorems 10 and 11. The time complexity is again dominated by Jordan decomposition used in computing $\mathcal{E}_\infty(\rho)$ and $\mathcal{E}_\infty(G^\perp)$, thus it is $O(n^8)$. □